Email Threat Review
Juli 2022

HORNETSECURITY

In diesem monatlichen Bericht über E-Mail-Bedrohungen geben wir einen Überblick über die im Juli 2022 beobachteten E-Mail-Bedrohungen und vergleichen sie mit den Bedrohungen des Vormonats. Der Bericht bietet Einblicke in:

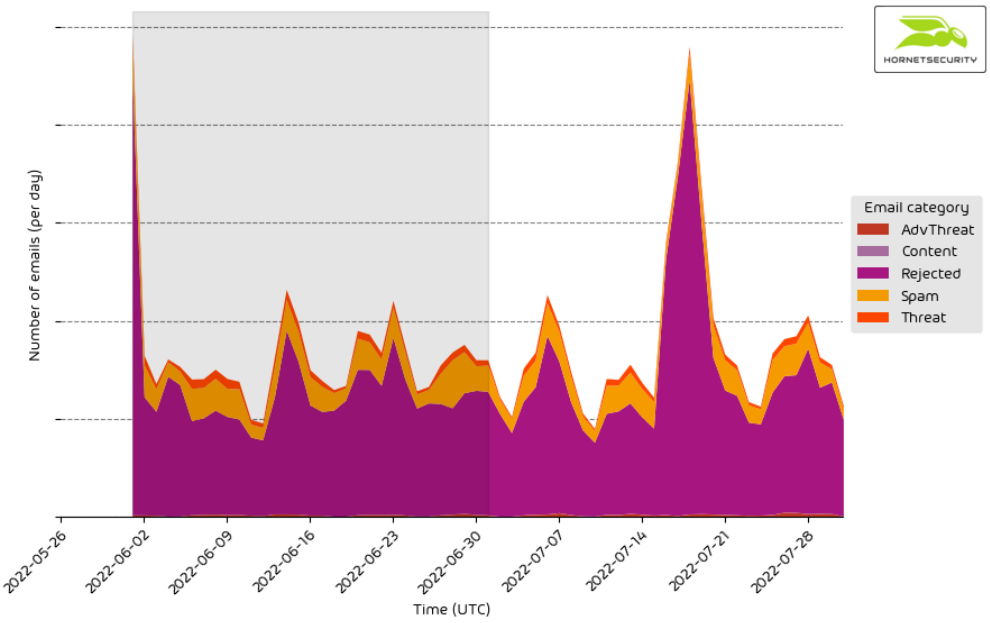
Inhalt

Unerwünschte E-Mails nach Kategorie

Die folgende Tabelle zeigt die Verteilung der unerwünschten E-Mails nach Kategorien.

E-Mail-Kategorie	%
Abgelehnt	82.11
Spam	13.42
Threat	3.02
AdvThreat	1.40
Content	0.05

Das folgende Zeithistogramm zeigt das E-Mail-Volumen pro Kategorie und Stunde.



Der Anstieg der abgelehnten E-Mails zwischen dem 17.07.2022 und dem 19.07.2022 kann auf eine Spam-Kampagne mit Sextortion zurückgeführt werden.

Methodik

Die aufgelisteten E-Mail-Kategorien entsprechen den E-Mail-Kategorien, die im Email Live Tracking des Hornetsecurity Control Panels aufgelistet sind. Unsere Benutzer sind also bereits mit ihnen vertraut. Für andere sind die Kategorien:

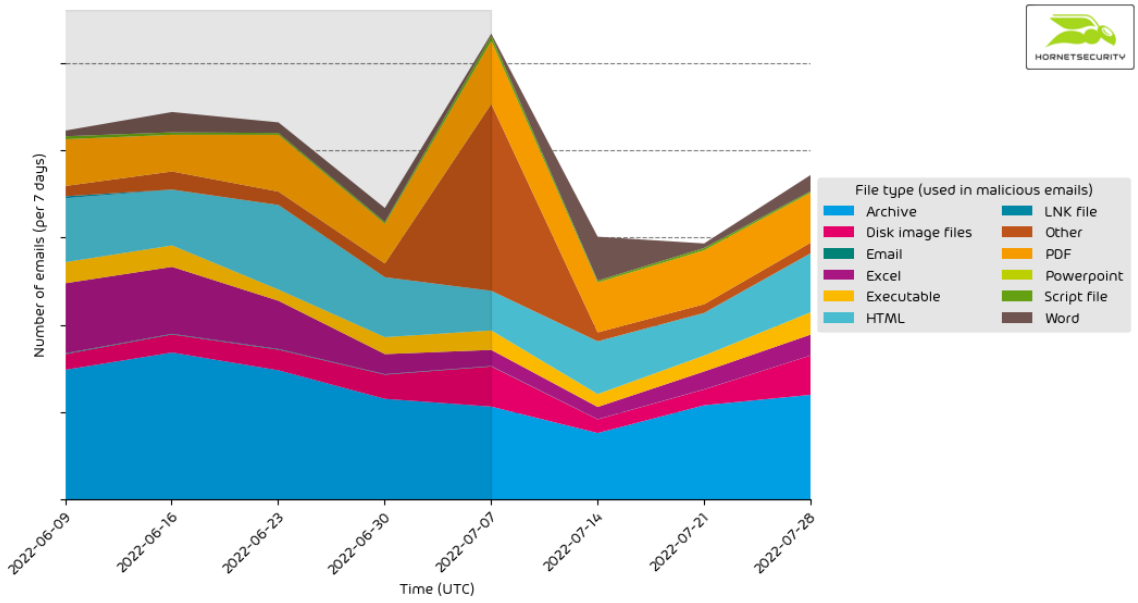
Kategorie	Beschreibung
Spam	Diese E-Mails sind unerwünscht und haben häufig einen werblichen oder betrügerischen Charakter. Die E-Mails werden gleichzeitig an eine große Anzahl von Empfängern verschickt.
Content	Diese E-Mails haben einen ungültigen Anhang. Welche Anhänge ungültig sind, legen die Administratoren im Modul Content Control fest.
Threat	Diese E-Mails enthalten gefährliche Inhalte wie bösartige Anhänge oder Links oder werden zur Begehung von Straftaten wie Phishing verschickt.
AdvThreat	Bei diesen E-Mails hat Advanced Threat Protection eine Bedrohung erkannt. Die E-Mails werden für illegale Zwecke eingesetzt und nutzen ausgeklügelte technische Mittel, die nur mithilfe von fortgeschrittenen dynamischen Verfahren abgewehrt werden können.
Abgelehnt	Diese E-Mails werden aufgrund externer Merkmale, die z. B. die Identität des Absenders betreffen können, im Laufe des SMTP-Dialogs direkt von unserem E-Mail-Server abgelehnt und nicht weiter analysiert.

Bei Angriffen verwendete Dateitypen

Die folgende Tabelle zeigt die Verteilung der in Angriffen verwendeten Dateitypen.

Dateityp (verwendet in bösartigen E-Mails)	%
Archive	27.5
PDF	16.5
HTML	14.8
Disk image files	8.3
Executable	5.4
Excel	5.1
Word	5.1
Script file	0.8
Other	16.4

Das folgende Histogramm zeigt das E-Mail-Volumen pro Dateityp, das bei Angriffen innerhalb von sieben Tagen verwendet wird.



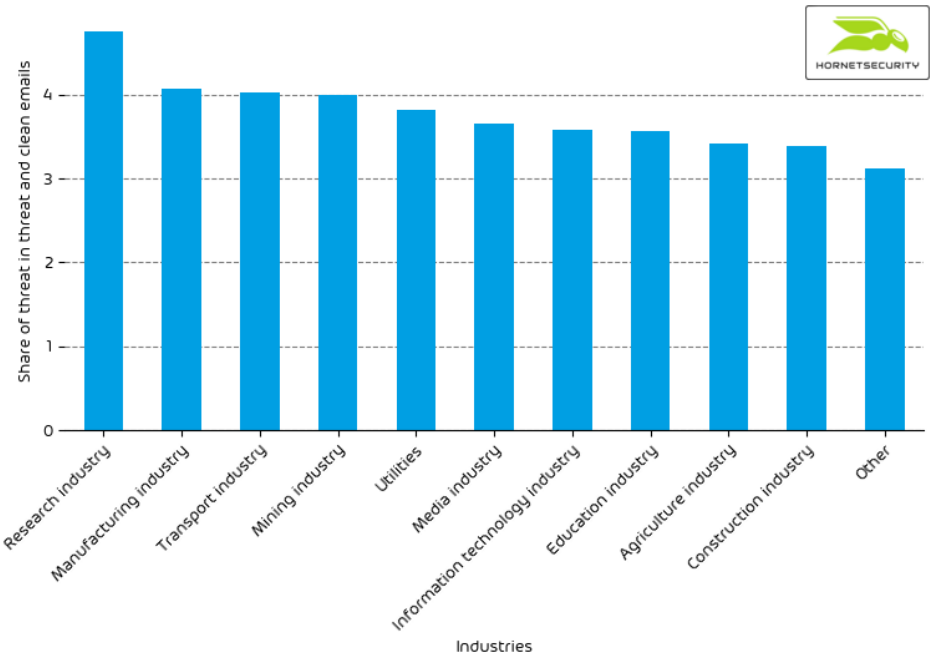
Der Rückgang der in Angriffen verwendeten Excel-Dokumente von 14,4 % auf 5,1 % kann darauf zurückgeführt werden, dass die Angreifer ihre Taktik aufgrund der Maßnahmen von Microsoft, Excel 4.0-Makros standardmäßig zu deaktivieren, geändert haben. Die bekannteste Malware, die über bösartige Excel 4.0-Makros verbreitet wurde, waren QakBot und Emotet. QakBot ging zu einer komplexen Infektionskette über, bei der HTML-Schmuggel und DLL-Side-Loading zum Einsatz kommen, worauf wir später in diesem Bericht eingehen.

Branchen Email Threat Index

Die folgende Tabelle zeigt unseren Branchen-E-Mail-Bedrohungsindex, der auf der Anzahl der schadhaften E-Mails im Vergleich zu den gültigen E-Mails der einzelnen Branchen (im Median) basiert.

Branchen	Anteil der Threat Emails an Threat und Gültigen Emails
Research industry	4.8
Manufacturing industry	4.1
Transport industry	4.0
Mining industry	4.0
Utilities	3.8
Media industry	3.7
Information technology industry	3.6
Education industry	3.6
Agriculture industry	3.4
Construction industry	3.4

Das folgende Balkendiagramm visualisiert die E-Mail-basierte Bedrohung für jede Branche.



Obwohl der Branchen Email Threat Index für die Forschungsbranche von 7,2 auf 4,8 gesunken ist, liegt sie immer noch an der Spitze. Allerdings liegt sie jetzt näher an der am zweithäufigsten bedrohten Fertigungsindustrie.

Methodik

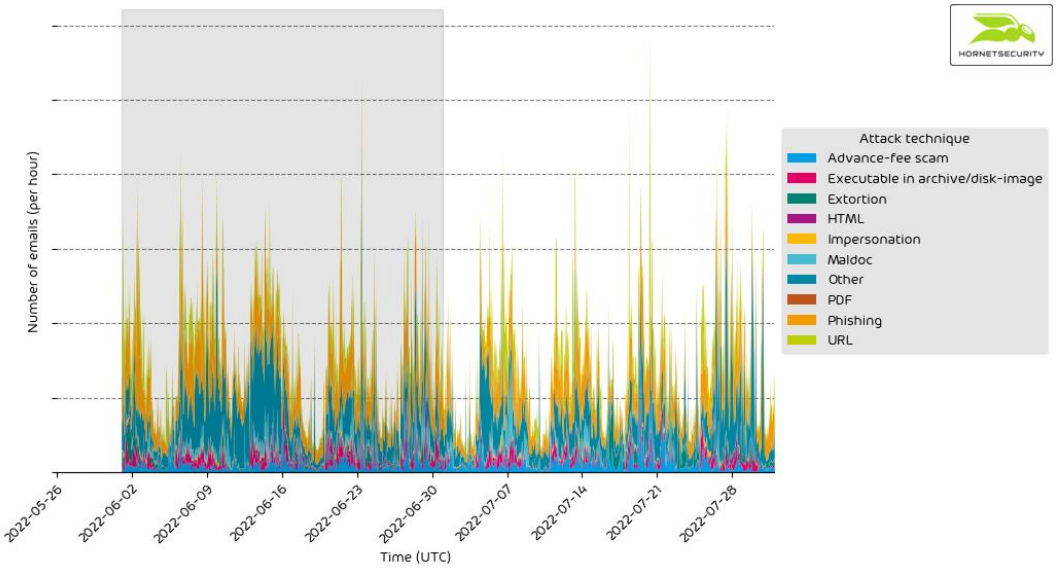
Unterschiedlich große Organisationen erhalten eine unterschiedliche absolute Anzahl von E-Mails. Um Organisationen zu vergleichen, haben wir daher den prozentualen Anteil der Threat E-Mails an den Threat und Gültigen E-Mails jeder Organisation berechnet. Anschließend berechnen wir den Median dieser Prozentwerte über alle Organisationen innerhalb derselben Branche, um den endgültigen Threat Index für die Branche zu ermitteln.

Angriffstechniken

Die folgende Tabelle zeigt die bei Angriffen verwendete Angriffstechnik.

Angriffstechnik	%
Phishing	29.4
URL	12.5
Advance-fee scam	9.4
Extortion	5.3
Executable in archive/disk-image	4.6
Maldoc	2.3
HTML	1.6
Impersonation	1.2
PDF	1.2
Other	32.4

Das folgende Zeithistogramm zeigt das E-Mail-Volumen pro eingesetzter Angriffstechnik pro Stunde.

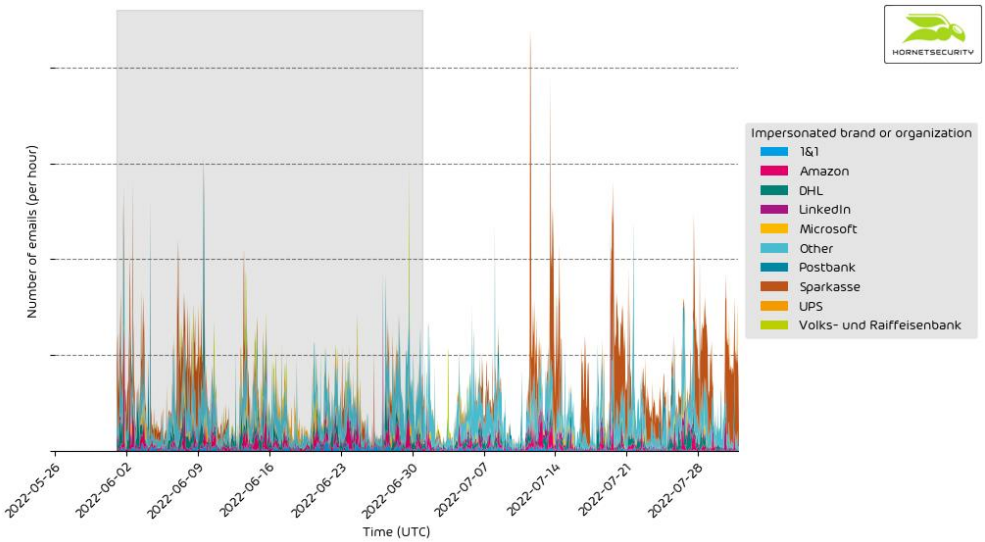


Imitierte Firmenmarken oder Organisationen

Die folgende Tabelle zeigt, welche Firmenmarken unsere Systeme am häufigsten bei Impersonationsangriffen entdeckt haben.

Imitierte Firmenmarke oder Organisation	%
Sparkasse	36.8
DHL	9.0
Amazon	6.7
LinkedIn	3.8
1&1	2.8
Postbank	2.8
Microsoft	2.4
Intuit	2.1
Mastercard	1.8
HSBC	1.5
American Express	1.5
DocuSign	1.5
UPS	1.3
Fedex	1.3
Strato	1.1
Volks- und Raiffeisenbank	0.9
Other	12.1

Das folgende Zeithistogramm zeigt das E-Mail-Volumen für Firmenmarken, die bei Impersonationsangriffen entdeckt wurden, pro Stunde.



In diesem Monat stieg Intuit, bekannt für seine Steuer- und Buchhaltungssoftware TurboTax und QuickBooks, von Platz 13 auf Platz 8 der bei Phishing-Angriffen am häufigsten imitierten Unternehmensmarken.

Hervorgehobene Bedrohungs-E-Mail-Kampagnen

QakBot wurde über eine komplexe Infektionskette verbreitet, bei der HTML-Smuggling und DLL-Side-Loading eingesetzt wurden, um die Entdeckung zu umgehen.

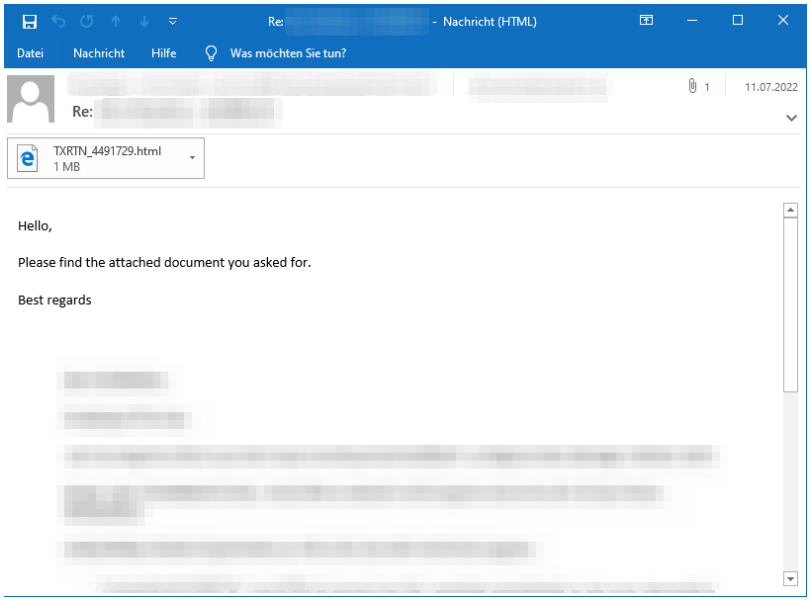
HTML-Smuggling nutzt HTML, um bösartige Inhalte in einem HTML-Anhang zu bündeln. Hornetsecurity hat bereits früher über HTML-Smuggling im Zusammenhang mit Phishing berichtet, bei dem die Phishing-Website vollständig in den HTML-Anhängen enthalten war.[1]

Bei der beobachteten QakBot-Kampagne werden E-Mails, die bösartige HTML-Dateien verbreiten, verwendet, um die QakBot-Malware auf den Computer des Opfers zu bringen, ohne dass ein zusätzlicher Download erforderlich ist, wie dies bei früheren QakBot-Angriffen auf der Basis von Excel-Dokumenten der Fall war.[3] Beim Empfang durch das Opfer wird die Malware aus dem HTML-Code erstellt, so dass zusätzliche Downloads in einem zweiten Schritt überflüssig sind und Unternehmen weniger Möglichkeiten haben, eine solche Malware-Infektion zu erkennen.

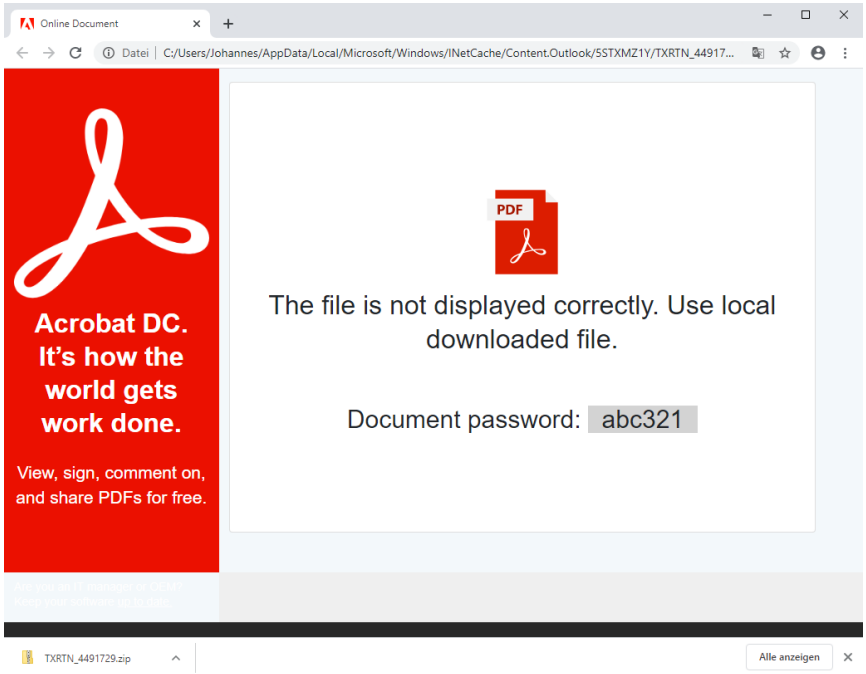
Zusätzlich zum HTML-Smuggling verwenden die Kampagnen eine Kette passwortgeschützter, verschlüsselter ZIP-Dateien, die eine ISO-Datei, eine LNK-Datei, zwei DLL-Dateien und eine legitime calc.exe-Binärdatei enthalten.

Die gesamte Kette funktioniert wie folgt:

Zuerst wird eine E-Mail mit einem HTML-Anhang empfangen, in der ein E-Mail-Konversations-Thread gekapert wurde mit einer Angriffstechnik die sich Email Conversation Thread Hijacking nennt.[2]

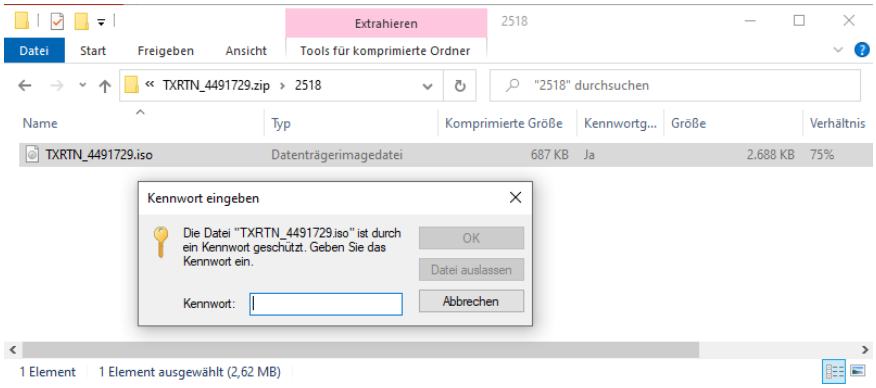


Der HTML-Anhang gibt vor, ein "Online Document" von Adobe zu sein, und fordert den Benutzer sofort zum Download auf.

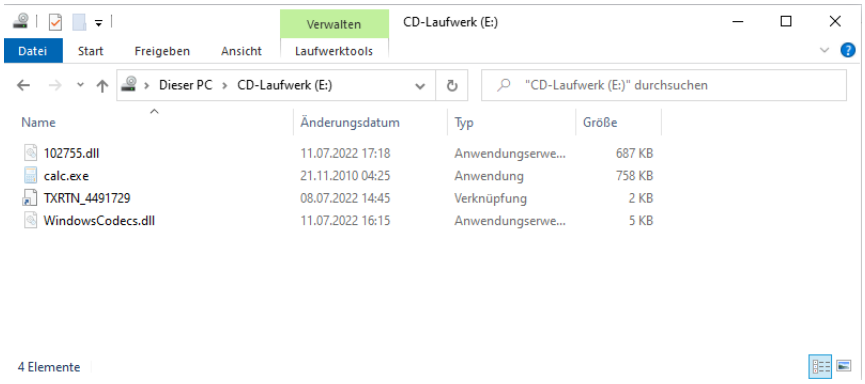


Der Download der ZIP-Datei erfolgt über Javascript, wobei der Inhalt der ZIP-Datei innerhalb des HTML-Dokuments als base64 kodiert wird. Auf diese Weise wird keine zusätzliche Netzwerkkommunikation ausgelöst.

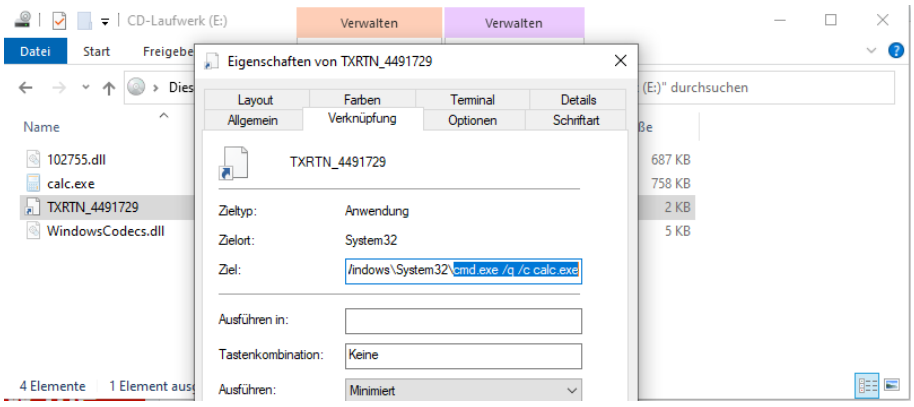
Außerdem wird im HTML-Dokument das Passwort angezeigt, das zur Entschlüsselung der ZIP-Datei benötigt wird.



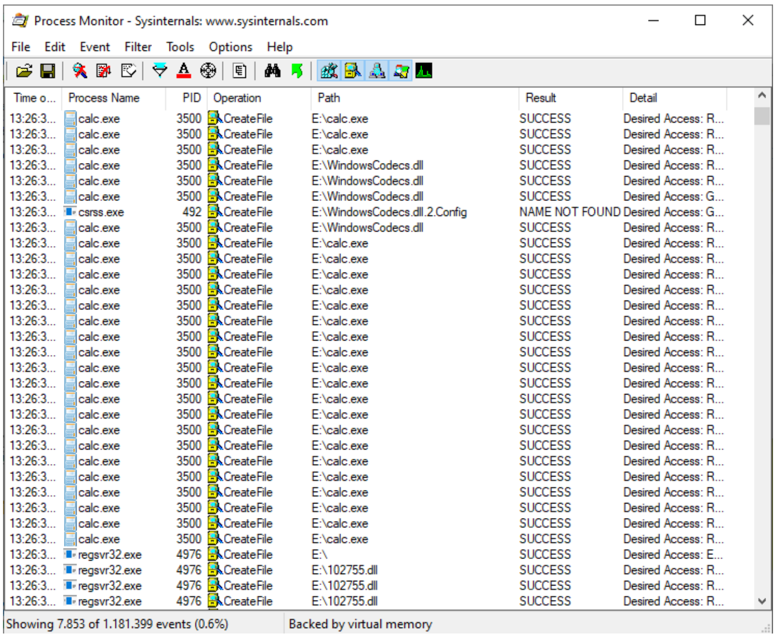
Die ZIP-Datei enthält eine ISO-Image-Datei, die zwei DLL-Dateien, eine LNK-Datei und eine legitime ausführbare Datei calc.exe.



Die LNK-Datei wird verwendet, um die legitime calc.exe aus dem Pfad innerhalb der eingebundenen ISO-Datei zu starten.



Die calc.exe wird dann verwendet, um eine der bösartigen DLLs mittels der sogenannten DLL-Side-Loading Technik zu laden. In dem in den Screenshots gezeigten Beispiel hat die geladene DLL den Namen WindowsCodecs.dll.



Diese erste DLL wird verwendet, um die eigentliche QakBot-Malware-DLL (in dem in den Screenshots gezeigten Beispiel mit dem Namen 102755.dll) über regsvr32.exe zu laden.

Methodik

Hornetsecurity beobachtet Tausende von Bedrohungs-E-Mail-Kampagnen unterschiedlicher Bedrohungsakteure, die von einfachen Angriffen mit geringem Aufwand bis hin zu hochkomplexen, verschleierten Angriffsschemata reichen. Unsere Hervorhebung umfasst nur eine Teilmenge dieser Bedrohungs-E-Mail-Kampagnen.

Querverweise

- [1] https://www.hornetsecurity.com/de/security-informationen/html-phishing-mit-doppelter-passwort-abfrage/
- [2] https://www.hornetsecurity.com/de/security-information-2/email-conversation-thread-hijacking/
- [3] https://www.hornetsecurity.com/de/threat-research/qakbot-verteilt-durch-xlsb-dateien/